CLAIMS

1. A method for providing node security in a router of a packet network, comprising the steps of:

monitoring a data packet sent from an originator via the router and addressed to a destination device other than the router;

determining in the router whether the data packet is potentially harmful to the destination device;

interrupting transmission of the data packet in response to determining that the data packet is potentially harmful to the destination device, comprising the step of communicating with a second router to cause the second router to interrupt transmission of a future data packet; and

transmitting the data packet in response to determining that the data packet is not potentially harmful to the destination device.

2. The method of claim 1, wherein the interrupting step comprises the step of discarding a later data packet from the originator.

3. The method of claim 1, wherein the interrupting step comprises the step of sending a command to an upstream router to intercept future data packets from the originator.

4. The method of claim 1, wherein the interrupting step comprises the step of forwarding an agent to an upstream router, the agent arranged to intercept future data packets from the originator.

5. The method of claim 1, wherein the determining step comprises the step of checking for a potential presence of at least one of a worm, a virus, and a Trojan horse.

6. The method of claim 1, wherein the monitoring step comprises at least one of the steps of:

random sampling of a subset of data packets;

monitoring data packets having a predetermined source address;

monitoring data packets having a predetermined destination address; and

monitoring data packets having a predetermined combination of source and destination address.

7. The method of claim 1, wherein the determining step comprises the steps of:

determining that a first data packet is suspicious; and

in response to determining that the first data packet is suspicious, deciding to monitor future data packets having at least one of a source address and a destination address matching, respectively, the source address and the destination address of the first data packet.

8. The method of claim 1, wherein the interrupting step comprises the step of collaborating with an upstream router to cause the upstream router to update its capabilities to detect a potentially harmful data packet.

9. The method of claim 1, wherein the interrupting step comprises the step of collaborating with an upstream router that is not a neighbor of the router to have the upstream router block transmissions from the originator.

10. The method of claim of 9, wherein the interrupting step further comprises the step of identifying the upstream router by sending a command to the originator, the command requesting address information from participating routers.

11. A router for providing node security in a packet network, comprising:

a plurality of I/O ports for accepting a data packet sent from an originator via the router and addressed to a destination device other than the router, and for transmitting the data packet to the destination device; and

a processor coupled to the plurality of I/O ports for processing the data packet;

wherein the processor is programmed to:

monitor the data packet;

determine whether the data packet is potentially harmful to the destination device;

interrupt transmission of the data packet in response to determining that the data packet is potentially harmful to the destination device, including communicating with a second router to cause the second router to interrupt transmission of a future data packet; and

transmit the data packet in response to determining that the data packet is not potentially harmful to the destination device.

12. The router of claim 11, wherein, in response to interrupting the data packet, the processor is further programmed to discard a later data packet from the originator.

13. The router of claim 11, wherein, in response to interrupting the data packet, the processor is further programmed to send a command

to an upstream router to intercept future data packets from the originator.

14. The router of claim 11, wherein, in response to interrupting the data packet, the processor is further programmed to forward an agent to an upstream router, the agent arranged to intercept future data packets from the originator.

15. The router of claim 11, wherein the processor is further programmed to check for a potential presence of at least one of a worm, a virus, and a Trojan horse.

16. The router of claim 11, wherein the processor is further programmed to at least one of:

random sample a subset of data packets;

monitor data packets having a predetermined source address;

monitor data packets having a predetermined destination address; and

monitor data packets having a predetermined combination of source and destination address.

17. The router of claim 11, wherein the processor is further programmed,

in response to determining that a first data packet is suspicious, to decide to monitor future data packets having at least one of a source address and a destination address matching, respectively, the source address and the destination address of the first data packet.

18. The router of claim 11, wherein the processor is further programmed to collaborate with an upstream router to cause the

upstream router to update its capabilities to detect a potentially harmful data packet.

19. The router of claim 11, wherein the processor is further programmed to collaborate with an upstream router that is not a neighbor of the router to have the upstream router block transmissions from the originator.

20. The router of claim of 19, wherein the processor is further programmed to identify the upstream router by sending a command to the originator, the command requesting address information from participating routers.